The Truth About Computer Scams

Steve Weisman

Trojan Horses

Keystroke logging programs, most commonly called Trojan horses, are a kind of spyware that, after installed on your computer, monitors all activity on your computer and transmits that information back to the scammer, who uses it to access your bank accounts, credit cards, brokerage accounts, or any of your online business. This information can even be used to establish credit in your name that the scammer will use without, of course, ever paying on the account, which then turns up as a black mark on your credit report and makes your life more

difficult.

The truth is Trojan horses are aptly named because they are installed in your computer by you when you unwittingly download them. A common way they reach your computer is an infected email with an attachment that installs the program onto your computer. Sharing of songs, games, or other material through peer-to-peer usage is another way that Trojan horses are stabled in your computer. To combat this threat, you must be more than cautious when downloading anything. Certainly, don't download anything from a source you're not entirely familiar with. Even downloading attachments from friends or family is no guarantee that your

computer won't be infected because the person may unintentionally be passing the Trojan horse on to you. The best course of action is to have a good firewall and antispyware software on your computer and keep the software constantly updated.

TIP A good firewall is an essential element in protecting your computer against keystroke logging programs. But, not all firewalls are created equal. Use a firewall, such as ZoneAlarm, which not only limits access to your computer, but also blocks unidentified programs on your computer from sending information back to the scammer who planted it, thereby minimizing the damage of a Trojan horse on your computer.

PayPal, eBay

If you have used eBay, the Internet auction site, you have probably used PayPal, which started as an independent company to help people pay for goods and services online and was bought by

eBay in 2002. A phishing scam starts with an email claiming to be from PayPal telling you that it has had some computer problems and it needs you to log on to your account to confirm your personal information. However, the link takes you to a phony PayPal website. If you go there and provide the information requested, you soon become a victim of identity theft.

Another PayPal scam involves an email that purports to be from PayPal informing you that you have received money from someone. (In many instances, the name used is Betty Hill, which interestingly enough, was the name of a woman who said she was abducted by aliens in New Hampshire in

1961.) You are then directed by a link to what looks like the official PayPal site, where you are asked to input your PayPal ID and password. If you do so, your PayPal account is now in the hands of scammers. If you have any thoughts that such a letter might be real, call PayPal.

Another common PayPal scam also starts with a phony email. This one confirms your payment of hundreds of dollars for a particular item you actually have not purchased. The email also indicates that if you have not authorized the particular charge, you can click on a link to cancel the payment and receive a full refund. This takes you to an official-looking website where you are required

to input personal information, including the number of any credit cards or debit cards used for your PayPal account. This is just another example of phishing used so that the scammer can get your personal information and access your accounts.

When using eBay and other online auctions, check out the references of the seller of anything you consider buying. Also, consider using an online escrow service. And, never provide information to PayPal or anyone else online unless you are absolutely positive of the identity of the person. Always be skeptical when PayPal or anyone else asks for information that they should already have.

Second Chances—eBay

Who doesn't like a second chance? Who wouldn't like a Mulligan? So when people receive an email telling them that they have another chance to bid on an item that they had lost out on because the winning eBay bidder failed to purchase the item, they are pleasantly surprised. Sometimes they are told that the winning bidder did not meet the reserve price, which is the minimum price set by the seller for sale of a particular item. What scammers do is wait until the end of an online auction and then look at the list of bidders and compose an email to losing bidders posing as the seller.

The phony email looks legitimate.

However, it asks for personal information to process the bid and receive an invoice from eBay. Unfortunately, after the victim provides his personal information, the invoice never comes. It is a scam that provides identity thieves important information about you. Another variation of this scam involves you being permitted to re-bid on an item and then being instructed to send in your winning bid by a wire transfer. After you send in your money by wire, the money is gone, but the item never comes.

The truth is although second chances do sometimes come in life and even in eBay, they do not come through emails directly from the seller of the item, but

rather from eBay itself. Sometimes the authentic second chance offer will come in an email from eBay with a Buy It Now icon you can click on to accept the offer. The email will also provide you with a new number and page for the item. Legitimate second chance offers also may appear as a link on the page of the particular listing. Below the message, “You were outbid” will appear any second chance opportunities. Second chance offers will also appear on your Items I Didn’t Win page on eBay. The truth is you should never consider emails for second chance offers that purport to be from the seller personally rather than from eBay. Never pay by a wire transfer, such as from Western Union or by a bank electronic transfer.

If there is a problem with the item, you have no recourse to get your money back if you have wired it. Finally, ignore messages that do not come to your eBay email account but rather turn up in your regular email.

Free Adult Entertainment

Pornography abounds on the Internet. Fully aware of the public's apparent never-ending appetite for online adult entertainment, enterprising scammers have used this to scam people out of money through their phone bills. A number of websites, such as the now shut-down sexygirls.com, were used in one particular scam to lure people by providing free Internet pornography that could be accessed only after

downloading what was referred to as a special “viewer” program. However, what the downloaded program actually did was disconnect the computer users from their local Internet service providers and reconnect the computers to a phone number in Moldova, an Eastern European country found between Romania and the Ukraine. Consequently, when the unwary computer user went to the adult entertainment websites promoted by the scammers, he incurred international telephone charges of more than $2 per minute. To make matters worse, the program did not disconnect the computer user from the international call until the computer was turned off. Thus, even after the computer user left

the particular adult entertainment website to do other online surfing, or even when the computer user was not on the Internet but merely using his computer for other purposes, such as word processing, the international call and the commensurate charges continued to accumulate so long as the computer was not turned off. The special “viewer” program also automatically turned off the computer user’s modem speakers so that the computer user would not hear the disconnect or the dialing of the international number. The lesson here is one not restricted to these particular pornographic websites. Do not download anything from a website you’re not familiar with and not

confident as to its legitimacy. In some instances, downloaded material may even contain Trojan horse, keystroke logging programs that can follow all your online activities and steal your passwords and personal information used online. This information, in turn, can be used to make you an identity theft victim.

Do not download anything from a website you're not familiar with and not confident as to its legitimacy.

If You Can't Trust Oprah

Oprah Winfrey is one of the most popular and trustworthy people in America today. So, if you got an email from Oprah, certainly you could believe that what she said was the truth—and

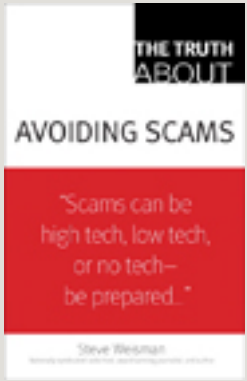
the information contained within that email probably would be information you could rely on. Unfortunately, for the many people who received an emailed invitation from Oprah to attend a taping of her show, the email they received was not from Oprah but from an identity thief. By the way, Oprah herself has been a victim of identity theft. It can happen to anyone. In the unsolicited email purporting to be from Oprah, the recipients were told that they would receive tickets to her show after they either verified financial information or wired money to a supplied address. As with all television shows, the Oprah Winfrey Show does not sell tickets. They are free. And, there would be no reason for Oprah to have anyone's

financial information. As always, the cardinal rule is: Never give your financial information to someone whom you have not contacted directly and whom you have not checked out for legitimacy.

From Russia, But Not With Love—The Hit Man Scam

Imagine how you would feel if you opened an email and found that it was a communication from a hit man saying that he has been hired to kill you by a "friend" of yours. Apparently, the hit man remembers the quote of Eddie Cantor, "He hasn't an enemy in the world—but all his friends hate him." Fortunately, however, the hit man goes on to tell you that after following you for some time, he has decided that if you

pay him a sum, typically ranging from $80,000 to $150,000, he will let you live. The FBI has tracked a number of these emails to Russia. They are a total scam. There is no hit man. The goal of the people behind this particular scam is to either get you to part with your money or induce you to provide them with personal information that can be used for identity theft. Either way, you lose. If you receive such an email, many of which have come from 1wayout@myway.com, report it to the FBI and the Internet Crime Complaint Center (IC3) at www.ic3.gov.



If you liked this Element, you might like the book by Steve Weisman, *The Truth About Avoiding Scams* (ISBN: 978-0-13-233385-6).

FT Press
FINANCIAL TIMES
Delivers

Vice President, Publisher: Tim Moore
Associate Publisher and Director of Marketing: Amy Neidlinger

Publishing as FTPress Delivers
Upper Saddle River, New Jersey 07458

ISBN-10: 0-13-265818-6
ISBN-13: 978-0-13-265818-8

For more information, please contact us at info@ftpress.com

FTPress Delivers Elements

An *e-burst* of inspiration for business and life.

31 Simple Rules for Protecting Your IRAs and 401(k)s

A quick, indispensable checklist for better retirement decision-making and financial planning—and a more secure, comfortable retirement!

Steve Weisman
ISBN: 978-0-13-703975-3
$1.99

Fighting Identity Theft!

Ten powerful new ways to prevent or respond to identity theft—techniques you haven't already heard!

Carolyn Warren
ISBN: 978-0-13-705053-6
$1.99

Establishing Goals for Living Rich

Setting and pursuing the goals that can

lead you to happiness—and, not coincidentally, lead you to financial security, too!

Farnoosh Torabi
ISBN: 978-0-13-261604-1
$1.99